



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/991,932	11/26/2001	Akiko Miyagawa	2565-0238P	9870

2292 7590 06/15/2007
BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER

NOBAHAR, ABDULHAKIM

ART UNIT	PAPER NUMBER
----------	--------------

2132

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

06/15/2007

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary	Application No.	Applicant(s)	
	09/991,932	MIYAGAWA ET AL.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 March 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-16 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This office action is in response to applicants' response filed on 03/29/2007.
2. Claims 1-16 are pending.
3. Claims 1 and 9 are amended.
4. Claim 17 is cancelled.
5. When responding to the Office action, Applicant is advised to clearly point out the patentable novelty the claims present in view of the state of the art disclosed by the reference(s) cited or the objection made. A showing of how the amendments avoid such references or objections must also be present. See 37 C.F.R. 1.111(c).

Response to Arguments

1. Applicant's arguments have been fully considered but they are not persuasive.
2. Applicants on page 10 and 11 of the remarks argue:

"Therefore, Sheymov monitoring center, which the Office Action alleges is Applicants' claimed decoy server and data center, does not prepare a response with the origination information as in the claims of the present invention. In Sheymov this is prepared and attached by the analysis system an intrusion detection not by the monitoring center 140."

"Therefore, Sheymov alone or in combination with Osborne fail to teach or suggest, inter alia, a decoy server functionally coupled to the control system, wherein the apparatus is placed outside an internal communication network."

"Sheymov and Osborne fail to teach, inter alia, taking internal measures against the illegal access data received by a data center remotely located from the internet from the

internal network, and the countermeasures include providing a response pretending to originate from the internal communication network, response being encapsulated by the data center and sent to a network device within the internal communication network to be decapsulated and transmitted by the network device to the communication device, as recited in claim 9.”

“Also, Sheymov and Osborne fail to teach, inter alia, receiving an encapsulated unauthorized access packet at a data center placed outside the internal network ...”

Examiner respectfully disagrees and asserts that Sheymov discloses a method for protecting a network that upon detection of an unauthorized access attempt by a hacker (Fig. 2, box 110) redirects the unauthorized access attempt to an analysis system and a monitoring center located outside the protected network (Fig. 2, boxes 120 and 140; paragraph [0036]) for handling. The monitoring center covertly (i.e., pretending) sends information to the analysis system removing the origin information of the monitoring center and the analysis center in turn forwards the information to the hacker that includes the origin information of the original target ([0036]). The hacker would see the information as if it has been truly sent from the intended target. Sheymov is quiet about encapsulation and decapsulation of the information transmitted between the monitoring system and the intrusion detection system. Osborne discloses a system for protecting a network that employs a host decoy (col. 2, lines 27-51; col. 4, lines 8-25) and encapsulates the transmitted data between the host decoy and the protected network (col. 2, lines 32-51; col. 6, lines 53-67). Hence, the combination of Sheymov

and Osborne teachings would meet the limitations of the independent claims 1, 9 and 13 of the instant invention.

3. Examiner, however, in light of the above submission maintains the previous rejections while considering the amendments to the claims 1 and 9 as follows:

Claim Objections

Claim 13 is objected to because of the following informalities: Claim 13, in line 2 recites "responding to unauthorized access to an internal". It is suggested that the claim 13 be amended in line 2 to recite "responding to an unauthorized access packet to an internal". Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sheymov et al (2002/0023227 A1; hereinafter Sheymov) in view of Osborne et al (6,687,833 B1; hereinafter Osborne).

Claims 1, 9 and 13

Sheymov discloses:

A control system (see, for example, Figs. 1 and 2, box 120, where the analysis system corresponds to the recited control system);

a decoy server, functionally coupled to the control system, wherein the apparatus is placed outside a given internal communication network (see, for example, Figs. 1 and 2, box 140; [0030]-[0031], where the monitoring system corresponds to the recited decoy server);

receiving an unauthorized access packet at a data center placed outside the internal network, and wherein the unauthorized access packet is redirected from a target server residing within the internal network (see, for example, Figs. 1 and 2, boxes 110, 120, 140 and 150; [0032]-[0037] and [0047]);

unauthorized access packet transmitted from a data communication device placed outside the internal communication network for a purpose of illegally accessing the internal communication network (see, for example, Figs. 1 and 2, boxes 13, 140 and 150; [0032]-[0037], where the hacker corresponds to the recited data communication device);

analyzing the received packet to formulate a response packet (see, for example, [0038]);

sending the response packet to the network device, wherein the network device is within the internal network to be transmitted by the network device to said data communication device (see, for example, Figs. 1 and 2, boxes 110, 120, 140 and 150;

[0032]-[0037] and [0047], where the monitoring system 140 generates a response and sends via analysis system 120 and intrusion detection system 110 to the hacker 150).

taking countermeasures against the illegal access data received, further wherein the countermeasures include providing a response pretending to originate from the internal communication network (see, for example, Figs. 1 and 2, [0014]-[0015], [0032]-[0037] and [0047]);

Sheymov does not expressly disclose that the illegal access data handling apparatus includes a capsulation section for decapsulating the encapsulated illegal access data received by the data reception section to extract the illegal access data, and encapsulates the response data.

Osborne, however, discloses a system for protecting an internal network from attacks originated from entities located in an external network (see Fig. 1; col. 1, lines 37-49). Osborne further discloses a capsulation mechanism deployed in the security components that encapsulate a response to an attacker before transmission (see col. 2, lines 28-51; col. 5, lines 1-11; col. 6, lines 53-67). Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to implement a capsulation mechanism as taught in Osborne in the system of Sheymov, because it would enable the security components of the protected system to decapsulate the receiving recursively encapsulated frames and encapsulate the response to an attacker (see Osborne, col. 2, lines 32-50).

Claims 2 and 10

Sheymov discloses:

The illegal access data handling apparatus of claim 1, wherein the illegal access data handling apparatus is connected to an illegal access data detection device for relaying a data communication between a data communication device placed within the internal communication network and a data communication device placed outside the internal communication network (see, for example, Figs. 1 and 2, boxes 110, 120, 140 and 150; [0032]-[0037] and [0047]).

Claims 3 and 11

Sheymov discloses:

The illegal access data handling apparatus of claim 2, further comprising:

a data reception section for receiving the illegal access data from the illegal access data detection device (see, for example, Figs. 3 and 4, [0039]-[004] and [0047]);

a data analysis section for analyzing the illegal access data received by the data reception section (see, for example, Figs. 3 and 4, [0039]-[004] and [0047]);

a response data generation section for generating response data to the illegal access data based upon an analysis result from the data analysis section (see, for example, Figs. 3 and 4, [0039]-[004] and [0047]); and

a data transmission section for transmitting the response data generated by the response data generation section to the illegal access data detection device (see, for example, Figs. 3 and 4, [0039]-[004] and [0047]).

Claim 4

Sheymov discloses:

The illegal access data handling apparatus of claim 3, wherein the data reception section receives an illegal access data from the illegal access data detection device (see col. 5, lines 55-61; col. 16, lines 15-20), and wherein the data transmission section transmits the response data to the illegal access data detection device (see, for example, Figs. 3 and 4, [0039]-[004] and [0047]),

Sheymov does not expressly disclose that the illegal access data handling apparatus includes a capsulation section for decapsulating the encapsulated illegal access data received by the data reception section to extract the illegal access data, and encapsulates the response data.

Osborne, however, discloses a system for protecting an internal network from attacks originated from entities located in an external network (see Fig. 1; col. 1, lines 37-49). Osborne further discloses a capsulation mechanism deployed in the security components that encapsulate a response to an attacker before transmission (see col. 2, lines 28-51; col. 5, lines 1-11; col. 6, lines 53-67). Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to implement a capsulation mechanism as taught in Osborne in the system of Sheymov, because it would enable the security components of the protected system to decapsulate the

receiving recursively encapsulated frames and encapsulate the response to an attacker (see Osborne, col. 2, lines 32-50).

Claims 5 and 12

Sheymov discloses:

The illegal access data handling apparatus of claim 3, wherein the response data generation section generates response data having same contents as those of response data that would be generated by a specific data communication device placed in the internal communication network in response to the illegal access data if the specific data communication device received the illegal access data (see, for example, abstract, [0011], [0036] and [0049]).

Claims 5 and 12

Regarding claims 5 and 12, Rothermel does not disclose a decoy device to respond to an illegal access attempt by an unauthorized user (e.g. a hacker) with a response to have similar content as a true response.

Osborne teaches a system and a method deploying a network host decoy to protect a network against attack by illicit users (see abstract and col. 1, lines 38-49). Osborne further teaches that a deceptive response is sent to an attacker by a pseudo host to cause an illusion so that it appears as a real answer originating from a device at the protected network (see, for example, col. 4, lines 8-25).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to deploy a decoy device as taught in Osborne in the system of

Rothermel because it provide a mechanism for better deception and more convincing and realistic to a would-be attacker (Osborne, col. 2, lines 52-55).

Claim 6

The illegal access data handling apparatus of claim 3, wherein the data reception section receives from the illegal access data detection device communication history information indicating a communication history of the illegal access data detection device (see, for example, [0007] and [0044]),

wherein the data analysis section analyzes the communication history information received by the data reception section, and generates illegal access data designation information designating data transmitted from a given data communication device placed outside the internal communication network as the illegal access data based upon an analysis result of the communication history information (see, for example, [0007] and [0042]-[0044]), and

wherein the data transmission section transmits the illegal access data designation information generated by the data analysis section to the illegal data detection device (see, for example, abstract, [0042]-[0044]).

Claim 7

Sheymov discloses:

The illegal access data handling apparatus of claim 4, wherein the data reception section receives the illegal access data having authentication information attached to be

Art Unit: 2132

used for data authentication from the illegal access data detection device, and wherein the capsulation section performs the data authentication for the illegal access data by using the authentication information (see, for example, [0030], where the analysis system verifies the access attempt).

Claim 8

Sheymov discloses:

The illegal access data handling apparatus of claim 7, wherein the capsulation section attaches the authentication information to be used for the data authentication for the response data to the response data, and wherein the data transmission section transmits the response data having the authentication information attached by the capsulation section to the illegal access data detection device (see, for example, [0036]).

Claim 14

Sheymov in view of Osborne discloses:

The method according to claim 13, further comprising:

determining if the encapsulated unauthorized access packet was transmitted from a client (see, for example, [0040] and [0044]);

judging whether data of the encapsulated unauthorized access packet came from an unauthorized source (see, for example, [0038]);

analyzing the encapsulated unauthorized access packet based upon data from a knowledge base (see, for example, [0043]); and
notifying a decoy server of the analysis result (see, for example, [0044]).

Claim 15

Sheymov in view of Osborne discloses:

The method according to claim 14, further comprising:
referring to a client database (see, for example, [0040] and [0044]); and
collating the encapsulated unauthorized access packet with information contained in the client database (see, for example, [0044] and [0050]).

Claim 16

Sheymov in view of Osborne discloses:

The method according to claim 14, further comprising:
accessing a knowledge base having information associated with past encapsulated unauthorized access packets (see, for example, [0043]-[0044]).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Abdulkhkim Nobahar
Examiner
Art Unit 2132 *A.N.*

June 10, 2007


KAMBIZ ZAND
SENIOR PATENT EXAMINER